#6

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicants: **MULLER, Frank; PRINS, Sharon Christie Lesley; ROELOFSEN, Gerrit**

International Application No.: **PCT/EP00/02617**

International Filing Date: **23 March 2000**

Priority Date Claimed: **01 April 1999**

Case: **PTT-124(402562US)**

Title: **METHOD FOR ENCIPHERING A SERIES OF SYMBOLS APPLYING A FUNCTION AND A KEY**

Commissioner for Patents
BOX PCT
Washington, D. C. 20231

S I R:

SUBMISSION OF PRIORITY DOCUMENT

In connection with the above-captioned application, applicants enclose the following certified priority document (with English translation) to support the claim to priority:

Netherlands Number 1011719, filed 01 April 1999.

Respectfully submitted,

25 September 2001

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & WALLACE
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

*****EXPRESS MAIL CERTIFICATION*****

"Express Mail" mailing label number: **EL632364856US**
Date of deposit: **26 September 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, **BOX PCT**, Washington, D.C. 20231.

Signature of person making certification

Peter L. MICHAELSON
Name of person making certification

(PTT124PRDOC/75:ca)

KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

Hierbij wordt verklaard, dat in Nederland op 1 april 1999 onder nummer 1011719,

ten name van:

KONINKLIJKE KPN N.V.

te Groningen

een aanvrage om octrooi werd ingediend voor:

"Werkwijze voor het met toepassing van een functie en een sleutel vercijferen van een reeks symbolen",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

CERTIFIED COPY OF PRIORITY DOCUMENT

Rijswijk, 25 januari 2000.

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

P.J.C. van den Nieuwenhuijsen.

Applicants: MULLER, Frank et al.
Atty. Doc. No.: PTT-124(402562US)
Title: METHOD FOR ENCIPHERING A SERIES OF SYMBOLS APPLYING A FUNCTION AND A KEY
Call: Peter L. Michaelson (732) 530-6671

09/937415
JC10 Rec'd PCT/PTO SEP 26 2001

U I T T R E K S E L

Werkwijze voor het met toepassing van een functie (8) en afhankelijk van een sleutelsymbolenreeks (4) vercijferen van een ingangssymbolenreeks (3) naar een uitgangssymbolenreeks (5, 20), waarbij voorafgaand aan het vercijferen de functie (8) afhankelijk van symbolen van de ingangssymbolenreeks (4) gewijzigd wordt.

Figuur 2

1011719

Korte aanduiding: Werkwijze voor het met toepassing van een functie en een sleutel vercijferen van een reeks symbolen.

De uitvinding heeft betrekking op een werkwijze volgens de aanhef van conclusie 1.

Een werkwijze van deze soort is bekend uit EP-A-0399587. Bij de bekende werkwijze bestaat de voor het vercijferen toegepaste functie uit een niet-lineaire functie die gevormd wordt door een substitutietabel ("S-box") die afhankelijk van de sleutel gegenereerd wordt. Het document geeft geen verdere beschrijving van de wijze waarop de substitutietabel gegenereerd wordt. Voor het verkrijgen van goede statistische eigenschappen van de uitvoer van de substitutietabel ten opzichte van variabele invoer wordt een door toepassing van de substitutietabel verkregen reeks symbolen gecombineerd met een even lange reeks van statistisch goed gespreide symbolen. De reeks symbolen die daarbij verkregen wordt kan gebruikt worden voor het vercijferen van een te vercijferen ingangssymbolenreeks in een vercijferde uitgangssymbolenreeks. Door toepassing van een sleutelafhankelijke substitutietabel in plaats van een vaste substitutietabel wordt het vercijferingsalgoritme versterkt.

De bekende werkwijze heeft als bezwaar dat wanneer in hoofdzaak steeds dezelfde sleutel gebruikt wordt de genoemde versterking van het vercijferingsalgoritme in de praktijk aanzienlijk teniet gedaan wordt. Dit kan zich bijvoorbeeld voordoen bij autenticatie bij gebruik van een chipkaart, zoals een telefoonkaart en een GSM-kaart.

De uitvinding beoogt de bezwaren van de bekende werkwijze op te heffen. Daartoe verschaft de uitvinding een werkwijze als beschreven in conclusie 1.

De verzender van de vercijferde uitgangssymbolenreeks en de ontvanger van deze reeks moeten beide de beschikking hebben over dezelfde sleutel en de voor het vercijferen gebruikte ingangssymbolenreeks, althans het gedeelte van laatstgenoemde reeks dat gebruikt werd voor het wijzigen van

de functie. Hierdoor is de werkwijze in het bijzonder geschikt voor authenticatie, waarbij de ontvanger van een vercijferde symbolenreeks kan controleren of een verzender met een aan de ontvanger gesuggereerde identiteit een bijpassende sleutel gebruikt heeft en bij een positieve uitkomst van deze controle de identiteit van de verzender voor de ontvanger verzekerd is.

De symbolenreeks die gebruikt wordt voor het wijzigen van de functie is in het bijzonder variabel en is bijvoorbeeld een per sessie opgewekt uitdaaggetal ("challenge number"), een (ander) willekeurig getal, of een variabele attribuut van de verzender, zoals een op een chipkaart bijgehouden saldo.

Wanneer de voor het vercijferen gebruikte niet-lineaire functie een inverteerbare functie was kan de ontvanger van de vercijferde symbolenreeks de genoemde controle uitvoeren met gebruik van dezelfde functie, dezelfde sleutel en de ontvangen symbolenreeks als invoer voor de functie. Het resultaat moet gelijk zijn aan de voor het vercijferen gebruikte ingangssymbolenreeks.

Omdat de ontvanger de bij het vercijferen gebruikte ingangssymbolenreeks kent kan de ontvanger de controle ook uitvoeren door dezelfde bewerkingen uit te voeren als door de verzender gedaan zijn, waarbij de door de ontvanger ontvangen reeks gelijk moet zijn aan de door de ontvanger opgewekte reeks. In dat geval is het geen eis dat de functie een inverteerbare functie is, waardoor bij gelijk blijvende complexiteit een sterker vercijferingsalgoritme gerealiseerd kan worden dat beter bestand is tegen aanvallen.

De voor het vercijferen toegepaste functie is bij voorkeur een niet-lineaire functie die gevormd kan worden door een substitutietabel of een cryptografische functie, zoals een functie waarbij afhankelijk van de invoer en de sleutel bepaalde bewerkingen al of niet uitgevoerd worden.

Verdere eigenschappen en voordelen van de uitvinding zullen blijken uit de hierna volgende toelichting van uitvoeringsvormen van de uitvinding in combinatie met de bijgevoegde tekeningen, waarin:

fig. 1 een schema toont van een bekend vercijferingsalgoritme;

fig. 2 een schema toont van een eerste uitvoeringsvorm van de uitvinding;

fig. 3 een stroomdiagram toont voor de werking van de uitvoeringsvorm volgens fig. 2; en

fig. 4 een andere uitvoeringsvorm van de uitvinding toont.

In fig. 1 is door middel van een blok 1 een bekend vercijferingsalgoritme (of encryptie-algoritme) voorgesteld. Het vercijferingsalgoritme maakt gebruik van één of meer, eveneens door blokken voorgestelde functies 2. Uitgaande van een te vercijferen ingangssymbolenreeks IN 3 bepaalt het vercijferingsalgoritme met behulp van een geheime sleutel 4 een vercijferde uitgangssymbolenreeks UIT 5. Het bekende vercijferingsalgoritme DES werkt volgens dit principe, waarbij acht niet-lineaire functies gebruikt worden die gevormd worden door substitutietabellen ("S-boxes"). De uitvinding is echter niet beperkt tot het DES algoritme en is ook niet beperkt tot het gebruik van niet-lineaire functies en van substitutietabellen voor de functies.

Fig. 2 toont een schema van een op het vercijferingsalgoritme van fig. 1 gebaseerd vercijferingsalgoritme 7 volgens de uitvinding. De functies zijn aangegeven met verwijzingscijfer 8. De functies 8 zijn te wijzigen door toepassing van een bijbehorend wijzigingsalgoritme 9 op basis van de ingangssymbolenreeks IN 3 of een gedeelte daarvan. De wijzigingsalgoritmen 9 hoeven niet gelijk te zijn.

Hierna zal met verwijzing naar het stroomdiagram van fig. 3 de werking van het vercijferingsalgoritme van fig. 2 toegelicht worden.

Een wijzigingsalgoritme 9 wijzigt de functie 8 op basis van een wijzigingssymbolenreeks die initieel van de ingangssymbolenreeks IN 3 afgeleid wordt (blok 11). Het wijzigen van de functie 8 vindt plaats in een aantal stappen, te weten de stappen n = 0 t/m n = Nmax, waarbij Nmax vast of ook afhankelijk van bijvoorbeeld de reeks IN 3 kan zijn. Daarom wordt bij aanvang van het wijzigen van de functie 8 een stappenteller

naar 0 geïnitialiseerd (blok 12). Vervolgens wordt de functie 8 op basis van de waarde van n en de wijzigingsreeks gewijzigd (blok 13). Vervolgens wordt het aantal getelde stappen met 1 verhoogd (blok 14). Vervolgens wordt gecontroleerd of de functie 8 reeds het maximum aantal keren gewijzigd is (blok 15). Wanneer aan deze voorwaarde voldaan is is het wijzigen van de functie 8 ten einde en anders wordt de wijzigingssymbolenreeks gewijzigd (stap 16) en wordt op basis van de nieuwe waarde van n en de gewijzigde wijzigingssymbolenreeks de functie 8 opnieuw gewijzigd (stap 13). In de hierna volgende Tabel I is een voorbeeld gegeven voor de werking van het in fig. 2 getoonde vercijferingsalgoritme 7.

TABEL I

stap n	wijzigings-symbolenreeks voor n>0 x(2) : = (x(0) + x(1)) mod8			vanaf stap n = 0 verwissel y(nmod8) en y(x(0))							
	x(0)	x(1)	x(2)	i	0	1	2	3	4	5	6	7
				y(i)	3	0	5	7	6	4	1	2
0	5	2	3	4	0	5	7	6	3	1	2
1	2	3	7	4	5	0	7	6	3	1	2
2	3	7	5	4	5	7	0	6	3	1	2
3	7	5	2	4	5	7	2	6	3	1	0
4	5	2	4	4	5	7	2	3	6	1	0
5	2	4	7	4	5	6	2	3	7	1	0
6	4	7	6	4	5	6	2	1	7	3	0
7	7	6	3	4	5	6	2	1	7	3	0
8	6	3	5	1	5	6	2	4	7	3	0
9	3	5	1	1	2	6	5	4	7	3	0

Er wordt aangenomen dat de symbolenverzameling acht

symbolen omvat, die in de Tabel weergegeven zijn met de cijfers 0 t/m 7. Verder wordt aangenomen dat de functie 8 gevormd wordt door een substitutietabel. Deze tabel kan gerealiseerd worden door een herschrijfbaar geheugen met acht geheugenlocaties met adressen of rangnummers i = 0...7. De geheugenlocaties bevatten elk een van de symbolen, waarbij elk symbool slechts eenmaal in de geheugenlocaties voorkomt. In Tabel I is de inhoud van een geheugenlocatie met adres of rangnummer i aangegeven met y(i). Initieel bevatten de geheugenlocaties voor i = 0...7 respectievelijk de symbolen 3, 0, 5, 7, 6, 4, 1, 2. Deze reeks symbolen vormt een initiële substitutietabel. Een symbool van een te vercijferen symbolenreeks wordt beschouwd als adres of rangnummer i en wordt vervangen door het symbool in de geheugenlocatie met dat adres. Volgens de initiële substitutietabel van Tabel I wordt dus bijvoorbeeld 0 vervangen door 3, 1 door 0, 2 door 5, ..., 7 door 2.

Alvorens een te vercijferen symbolenreeks vercijferd wordt, wordt volgens de uitvinding eerst de initiële substitutietabel gewijzigd. Volgens het voorbeeld van Tabel I gebeurt het wijzigen in tien stappen (stap n = 0 t/m n = Nmax). De wijziging vindt plaats afhankelijk van de symbolen van de te vercijferen symbolenreeks, althans van een aantal symbolen daarvan. In Tabel I zijn de te vercijferen symbolen die gebruikt worden voor het wijzigen van de substitutietabel de bij stap n = 0 aangegeven symbolen 5, 2 en 3. Deze symbolen worden toegewezen aan respectieve variabelen x(0), x(1) en x(2).

Tijdens de eerste stap met n = 0 wordt het symbool y(n), dat wil zeggen het symbool 3 van geheugenlocatie 0, verwisseld met het symbool y(x(0)), te weten symbool 4 van locatie x(0) =5. In Tabel I zijn voor de duidelijkheid voor elk van de tien stappen n = 0 ... 9 de verwisselde symbolen van de substitutietabel van acht symbolen onderstreept.

Vervolgens wordt een hulpvariabele h berekend die gelijk is aan:

h = (x(0) + x(1)) modulo (het aantal mogelijke symbolen), of in het voorbeeld

h = (x(0) + x (1)) modulo 8.

Vervolgens worden de symbolen van de wijzigingssymbolenreeks x(0), x(1) en x(2) als volgt vervangen (":=" betekent "wordt", dat wil zeggen een toewijzing).

x(0): = x(1),
x(1): = x(2), en
x(2): = h.

Het voor elke stap verwisselen van symbolen op basis van het stapnummer en de symbolen van de wijzigingssymbolenreeks wordt een geschikt aantal keren herhaald, in het voorbeeld van Tabel I Nmax + 1 = 10 keer. Aan het einde van dit wijzigingsalgoritme is de initiële substitutietabel:

3, 0, 5, 7, 6, 4, 1, 2

vervangen door een uiteindelijke substitutietabel:

1, 2, 6, 5, 4, 7, 3, 0.

Vervolgens kunnen de symbolen van een ingevoerde te vercijferen reeks in overeenstemming met de rangschikking van de symbolen in de uiteindelijke substitutietabel vervangen worden voor het leveren van een uitgaande vercijferde symbolenreeks. Hierdoor worden in het voorbeeld de reeks ingevoerde symbolen 5, 2, 3 vervangen door respectievelijk 7, 6, 5. Deze uitgaande symbolenreeks wordt voor eventuele verdere stappen van het vercijferingsalgoritme gebruikt.

Fig. 4 toont het schema van een vercijferingsalgoritme 18, dat van de vercijferingsalgoritme 5 van fig. 2 verschilt doordat het wijzigingsalgoritme 9 vervangen is door een wijzigingsalgoritme 19. Het wijzigingsalgoritme 19 is, net als het wijzigingsalgoritme 9, afhankelijk van een aantal te vercijferen symbolen IN 3, maar bovendien van een aantal symbolen van de sleutel 4.

Tabel II geeft een voorbeeld van de werking van het wijzigingsalgoritme 19.

TABEL II

stap n	wijzigings-symbolenreeks voor n>0 x(2):=(x(0) + x(1))mod8					vanaf stap n = 0 verwissel y(nmod8) en y(x(0))							
	x(0) x(1)		x(2) x(3)		x(4)	i	0	1	2	3	4	5	6	7
						y(i)	3	0	5	7	6	4	1	2
0	5	2	3	2	4		4	0	5	7	6	3	1	2
1	2	3	2	4	7		4	5	0	7	6	3	1	2
2	3	2	4	7	5		4	5	7	0	6	3	1	2
3	2	4	7	5	5		4	5	0	7	6	3	1	2
4	4	7	5	5	6		4	5	0	7	6	3	1	2
5	7	5	5	6	3		4	5	0	7	6	2	1	3
6	5	5	6	3	5		4	5	0	7	6	1	2	3
7	5	6	3	5	2		4	5	0	7	6	3	2	1
8	6	3	5	2	3		2	5	0	7	6	3	4	1
9	3	5	2	3	1		2	7	0	5	6	3	4	1

Tabel II verschilt van Tabel I slechts doordat de wijzigingssymbolenreeks x(0), x(1), x(2) aangevuld is met x(3), x(4). De symbolen x(3) en x(4) zijn afgeleid van de sleutel 4. In het voorbeeld van Tabel II is de initiële wijzigingssymbolenreeks 5, 2, 3, 2, 4. De uiteindelijke substitutietabel is volgens Tabel II:

2, 7, 0, 5, 6, 3, 4, 1.

De ingevoerde symbolenreeks IN 3 met de symbolen 5, 2, 3 wordt in overeenstemming met deze uiteindelijke substitutietabel vervangen door de vercijferde uitgangssymbolenreeks UIT 20 met de symbolen 3, 0, 5.

De symbolen van de initiële substitutietabel kunnen willekeurig gerangschikt zijn, zolang zowel de zender van een vercijferde symbolenreeks UIT 5 en de ontvanger van de vercijferde symbolenreeks dezelfde initiële substitutietabel gebruiken. Wanneer aan deze voorwaarde steeds voldaan kan

worden kan het vercijferingsalgoritme versterkt worden door als initiële substitutietabel een substitutietabel te gebruiken die tijdens een voorgaand vercijferingsproces gebruikt is, bijvoorbeeld de laatst gebruikte uiteindelijke substitutietabel. Wanneer het gevaar bestaat dat niet steeds aan de genoemde voorwaarde voldaan wordt, kan erin voorzien worden dat de ontvanger van de vercijferde symbolenreeks een aantal van dergelijke voorgaande substitutietabellen onthoudt en een oudere daarvan gebruikt wanneer het ontcijferen van de ontvangen reeks tot een negatief controleresultaat leidt.

Doordat zowel tijdens het vercijferen van een reeks symbolen als tijdens het ontcijferen daarvan de gebruikte sleutels gelijk moeten zijn en kennis aanwezig moet zijn van de vercijferde reeks symbolen IN 3 kan de ontvanger van de vercijferde reeks precies dezelfde bewerking, te weten een vercijfering, uitvoeren als de ontvanger gedaan heeft en de resultaten met elkaar vergelijken. In dat geval kan voor de functie een niet-inverteerbare functie gebruikt worden die, bij gelijk blijvende complexiteit, een sterker vercijferingsalgoritme mogelijk maakt.

De in combinatie met de Tabellen I en II toegelichte wijzigingsalgoritmen dienen slechts als voorbeeld. Voor het wijzigen van de wijzigingssymbolenreeks kunnen bijvoorbeeld voor elke stap meer dan twee en/of een verschillend aantal modulo optellingen toegepast worden en kunnen de symbolen van de wijzigingsreeks op andere wijzen geherrangschikt worden in plaats van door middel van een eenvoudige verschuiving.

C O N C L U S I E S

1. Werkwijze voor het met toepassing van een functie (2, 8) en afhankelijk van een sleutelsymbolenreeks (4) vercijferen van een ingangssymbolenreeks (3), omvattende:

het door middel van een wijzigingsalgoritme en afhankelijk van een wijzigingssymbolenreeks wijzigen van de functie;

het aan de gewijzigde functie onderwerpen van de ingangssymbolenreeks voor het afhankelijk van de sleutelsymbolenreeks bepalen van een uitgangssymbolenreeks (5, 20),

met het kenmerk, dat het wijzigingsalgoritme (9, 19) een aantal sequentiële stappen omvat, waarbij in elke stap de functie (8) afhankelijk van de wijzigingssymbolenreeks gewijzigd wordt en na elke stap de wijzigingssymbolenreeks door middel van een subalgoritme gewijzigd wordt, waarbij voor de eerste stap (n = 0) als wijzigingssymbolenreeks een initiële wijzigingssymbolenreeks gebruikt wordt die van de ingangssymbolenreeks (3) afgeleid wordt.

2. Werkwijze volgens conclusie 1, **met het kenmerk**, dat de initiële wijzigingssymbolenreeks tevens van de sleutelsymbolenreeks (4) afgeleid wordt.

3. Werkwijze volgens conclusie 1 of 2, **met het kenmerk**, dat het wijzigingsalgoritme (9, 19) het vervangen omvat van een symbool van de wijzigingssymbolenreeks door een vervangend symbool dat verkregen wordt door een optelling van twee of meer symbolen van de wijzigingssymbolenreeks modulo het aantal mogelijke verschillende symbolen.

4. Werkwijze volgens een voorgaande conclusie, **met het kenmerk**, dat het wijzigingsalgoritme (9, 19) het wijzigen van rangnummers omvat van twee of meer van de symbolen van de wijzigingssymbolenreeks.

5. Werkwijze volgens een voorgaande conclusie, **met het kenmerk**, dat voor het wijzigen van de functie als initiële

functie de functie gebruikt wordt die eerder gebruikt werd voor het bepalen van een eerdere uitgangssymbolenreeks (5, 20).

6. Werkwijze volgens een voorgaande conclusie, **met het kenmerk**, dat de functie een substitutiefunctie is.

7. Werkwijze volgens een van de conclusies 1 t/m 5, **met het kenmerk**, dat de functie een niet-inverteerbare functie is.

8. Werkwijze volgens een van de voorgaande conclusies, **met het kenmerk**, dat de functie een substitutietabel ("S"-box) omvat die vervangende symbolen voor de symbolen van de ingangssymbolenreeks bevat, en het wijzigingsalgoritme het afhankelijk van de wijzigingssymbolenreeks verwisselen van twee of meer symbolen van de substitutietabel omvat.

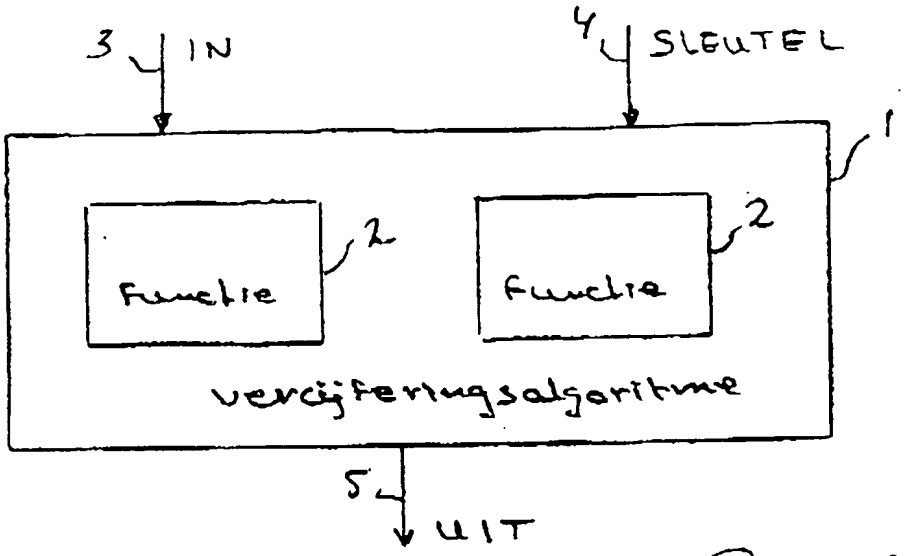
3
IN
4
SLEUTEL
1
Functie
2
Functie
2
verwijderingsalgoritme
5
UIT

Fig 1

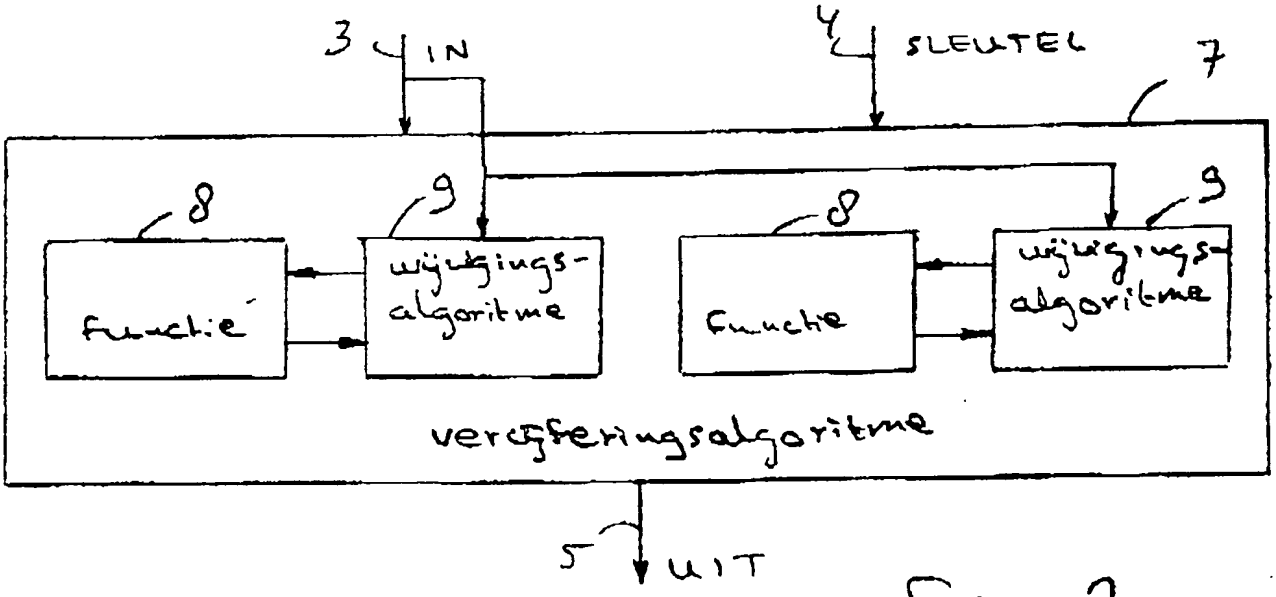
3
IN
4
SLEUTEL
7
8
9
Functie
wijzigings-
algoritme
8
9
Functie
wijzigings-
algoritme
verwijderingsalgoritme
5
UIT

Fig 2

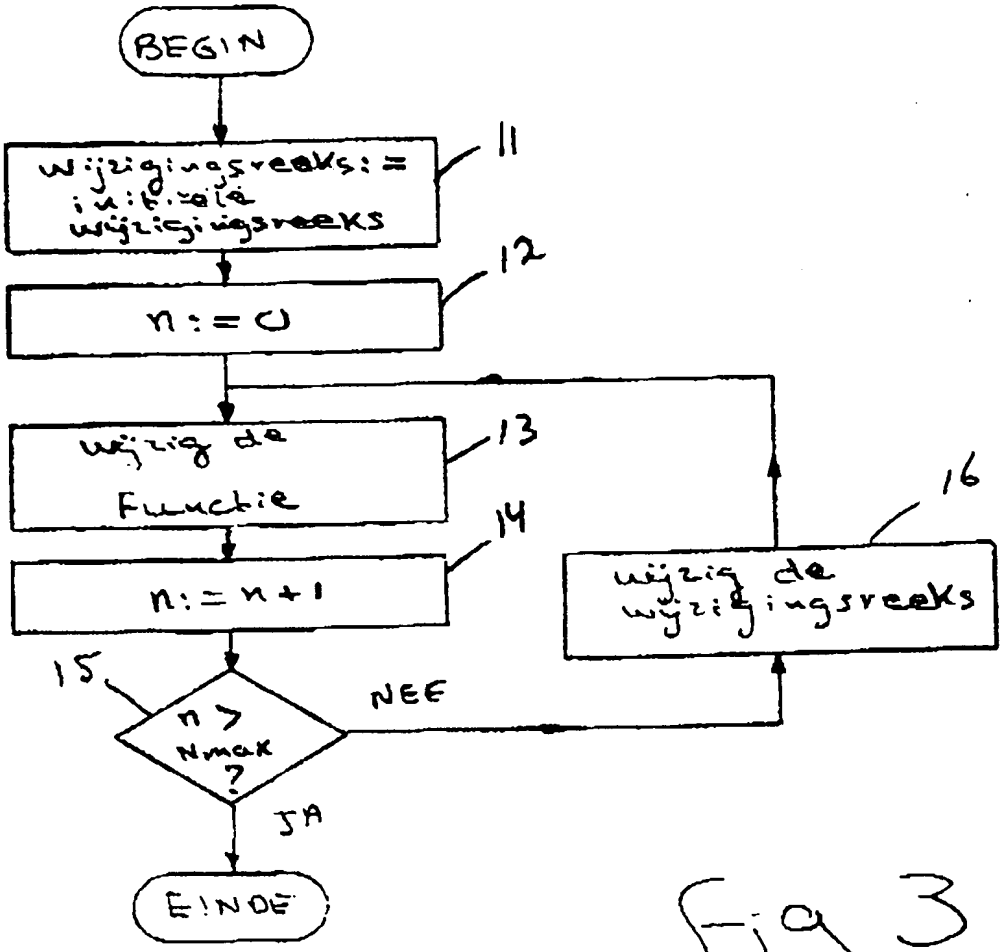
BEGIN
wijzigingsreeks := initiële wijzigingsreeks
11
n := 0
12
wijzig de Functie
13
n := n + 1
14
n > Nmax ?
15
NEE
JA
wijzig de wijzigingsreeks
16
EINDE

Fig 3

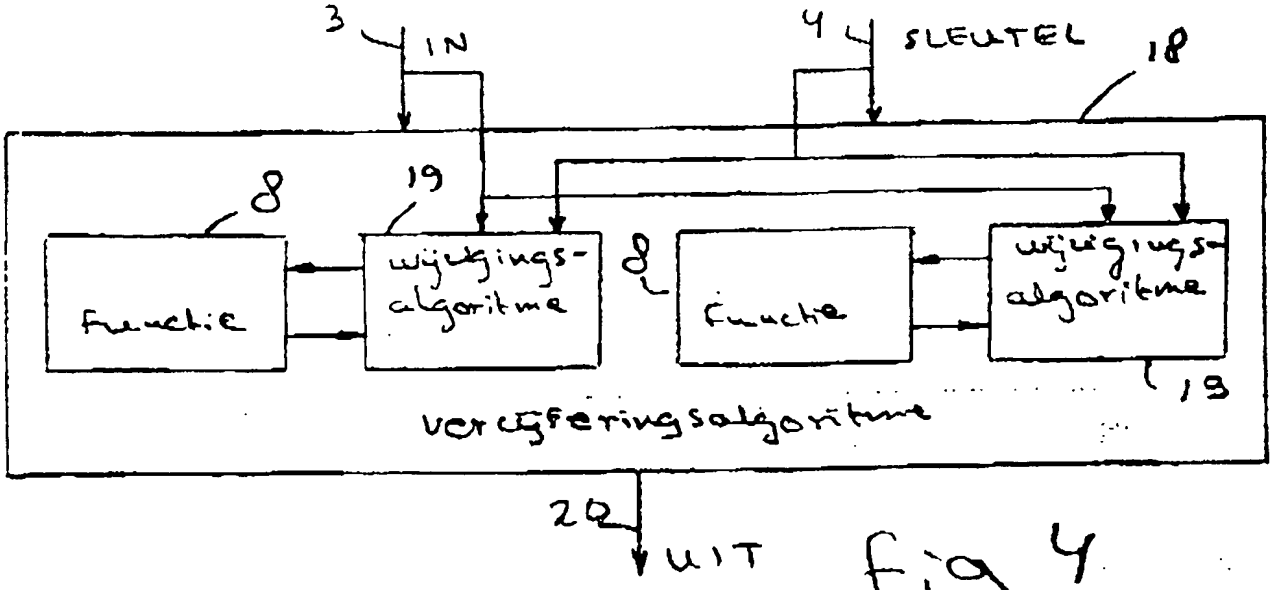
3
IN
4
SLEUTEL
18
8
19
Functie
wijzigings-algoritme
8
Functie
wijzigings-algoritme
19
verwerkingsalgoritme
20
UIT

Fig 4